

## ***Welcome to the PIA for FY 2011!***

Congress passed the E-Government Act of 2002 to encourage the use of Web-based Internet applications or other information technology by Government agencies, with the intention of enhancing access to government information and services and increasing the effectiveness, efficiency, and quality of government operations.

To combat public concerns regarding the disclosure of private information, the E-Government Act mandated various measures, including the requirement that Federal agencies conduct a Privacy Impact Assessment (PIA) for projects with information technology systems that collect, maintain, and/or disseminate "personally identifiable information" of the public. Personally identifiable information, or "personal information," is information that may be used to identify a specific person.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

### ***Directions:***

VA 6508 is the directive which outlines the PIA requirement for every System/Application/Program.

If you find that you can't click on checkboxes, make sure that you are: 1) Not in "design mode" and 2) you have enabled macros.

PIA Website: [http://vawww.privacy.va.gov/Privacy\\_Impact\\_Assessments.asp](http://vawww.privacy.va.gov/Privacy_Impact_Assessments.asp)

### ***Roles and Responsibilities:***

Roles and responsibilities for the specific process are clearly defined for all levels of staff in the VA Directive 6508 referenced in the procedure section of this document.

- a. The Privacy Officer is responsible for the overall coordination and review of the PIA to ensure compliance with VA Directive 6508.
- b. Records Officer is responsible for supplying records retention and deletion schedules.
- c. Information Technology (IT) staff responsible for the privacy of the system data will perform a PIA in accordance with VA Directive 6508 and to immediately report all anomalies to the Privacy Service and appropriate management chain.
- d. Information Security Officer (ISO) is responsible for assisting the Privacy Officer and providing information regarding security controls.
- e. The CIO is responsible for ensuring that the systems under his or her jurisdiction undergo a PIA. This responsibility includes identifying the IT systems; coordinating with the Privacy Officer, Information Security Officer, and others who have concerns about privacy and security issues; and reviewing and approving the PIA before submission to the Privacy Service.

### ***Definition of PII (Personally Identifiable Information)***

Information in identifiable form that is collected and stored in the system that either directly identifies an individual by name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique numbers, codes or characteristics or combined, indirect identify an individual such as a combination of gender, race, birth date, geographical indicators, license number is also considered PII.

### ***Macros Must Be Enabled on This Form***

**Microsoft Office 2003:** To enable macros, go to: 1) Tools > Macros > Security - Set to Medium; 2) Click OK; 3) Close the file and when reopening click on Enable Macros at the prompt.

**Microsoft Office 2007:** To enable macros, go to: 1) Office Button > Prepare > Excel Options > Trust Center > Trust Center Settings > Macro Settings > Enable All Macros; 2) Click OK

### ***Final Signatures***

Final Signatures are digitally signed or wet signatures on a case by case basis. All signatures should be done when all modifications have been approved by the VA Privacy Service and the reviewer has indicated that the signature is all that is necessary to obtain approval.

### ***Submitting PIA's into SMART***

#### ***Privacy Impact Assessment Uploaded into SMART***

Privacy Impact Assessments should be uploaded into C&A section of SMART.

All PIA Validation Letters should be emailed to [christina.pettit@va.gov](mailto:christina.pettit@va.gov) to received full credit for submission.

## (FY 2011) PIA: System Identification

Program or System Name: **REGION 4 > VHA > VISN 02 > BATH VAMC > LAN**  
OMB Unique System / Application / Program Identifier (AKA: UPID #): 029-00-02-00-01-1120-00

The LAN system is the hardware infrastructure on which the VHA health care facilities operate their software applications and support for E-Government initiatives to include Picture Archiving and Communication Systems (PACS). The PACS applications in VISN 2 LAN systems include radiology, cardiology, optometry and dental. Note that PACS is a generic term for anything that archives images. Radiology, Cardiology, Optometry, and Dental utilize PACS for their departments. It includes the computer equipment associated with clinical operations and the employees (approximately 2500 FTE) necessary to operate the system. LAN system supported IT services across the VA organization which had a network of 21 Veterans Integrated Service Networks (VISNs) that managed 155 medical centers, over 881 community based outpatient clinics, 46 residential rehabilitation treatment programs, 135 nursing homes, 207 readjustment counseling centers, 57 veteran benefits regional offices, and 125 national cemeteries. Using the LAN provides connectivity that supports the delivery of healthcare to veterans and their dependants. Using the computer, the VA health care provider can access applications and meet a wide range of health care data needs. The LAN system is in the mature phase of the capital investment lifecycle.

### Description of System/ Application/ Program:

Facility Name:	Bath VAMC, Bath, New York		
Title:	Name:	Phone:	Email:
Privacy Officer:	Jacquelyn Filkins	607-664-4823	<a href="mailto:Jacquelyn.Filkins@va.gov">Jacquelyn.Filkins@va.gov</a>
Information Security Officer:	Audrey Ross	607-664-4507	<a href="mailto:Audrey.Ross@va.gov">Audrey.Ross@va.gov</a>
System Owner/ Chief Information Officer:	Diane Niemann	518-626-6212	<a href="mailto:Diane.Niemann@va.gov">Diane.Niemann@va.gov</a>
Person Completing Document:	Denise Harrington-Nicita	315-425-6595	<a href="mailto:Denise.Harrington-Nicita@va.gov">Denise.Harrington-Nicita@va.gov</a>
Date of Last PIA Approved by VACO Privacy Services: (MM/YYYY)			07/2009
Date Approval To Operate Expires:			08/20011
What specific legal authorities authorize this program or system:			Title 38, United States Code, section 7301(a).
What is the expected number of individuals that will have their PII stored in this system:			1,000,000-9,999,999
Identify what stage the System / Application / Program is at:			Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.			Operational since approximately 1988
Is there an authorized change control process which documents any changes to existing applications or systems?			Yes
If No, please explain:			
Has a PIA been completed within the last three years?			Yes
Date of Report (MM/YYYY):			03/2011

**Please check the appropriate boxes and continue to the next TAB and complete the remaining questions on this form.**

- ☐ Have any changes been made to the system since the last PIA?
- ☒ Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?
- ☒ Will this system/application/program retrieve information on the basis of name, unique identifier, symbol, or other PII data?
- ☒ Does this system/application/program collect, store or disseminate PII/PHI data?
- ☒ Does this system/application/program collect, store or disseminate the SSN?

**2. System Identification**  
**If there is no Personally Identifiable Information on your system, please complete TAB 7 & TAB 12. ( See Comment for Definition of PII)**

(FY 2011) PIA: System of Records

Is the data maintained under one or more approved System(s) of Records? If the answer above  
no, please skip to row 15.

Yes

For each applicable System(s) of Records, list:

02VA135; 04VA115; 07VA138; 14VA135; 20VA138; 23VA163;  
24VA19; 28VA119; 29VA11; 32VA00; 33VA113; 34VA12; 54VA17;  
57VA10C2; 64VA15; 65VA122; 69VA131; 73VA14; 77VA10Q;  
79VA19; 84VA111K; 89VA19; 90VA194; 91VA111C; 93VA131;  
97VA105; 98VA104A; 99VA131; 100VA10NS10; 105VA131;  
106VA17; 108VA11S; 110VA10; 113VA112; 114VA16; 115VA10;  
117VA103; 121VA19; 130VA19

Applicants for Employment under Title 38, USC-VA; Blood Donor  
Information-VA; Department of Medicine and Surgery Engineering  
Employee Management Information Records-VA; Individuals Serving on  
a Fee Basis or without Compensation (Consultants, Attendings, Others)  
Personnel Records-VA; Motor Vehicle Operator Accident Records-VA;  
Non-VA Fee Basis Records-VA; Patient Medical Records-VA; Personnel  
Registration under Controlled Substance Act-VA; Physician, Dentist and  
Supervisory Nurse Professional Standards Board Action File-VA;  
Veteran, Employee and Citizen Health Care Facility Investigation Records-  
VA; National Prosthetics Patient Database-VA; Veteran, Patient,  
Employee and Volunteer Research and Development Project Records-  
VA; Health Administration Center Civilian Health and Medical program  
Records-VA; Voluntary Service Records-VA; Readjustment Counseling  
Service (RCS) Vet Center Program-VA; Community Placement Program-  
VA; Ionizing Radiation Registry-VA; Health Professional Scholarship  
Program-VA; Health Care Provider Credentialing and Privileging Records-  
VA; Veterans Health Information System and Technology Architecture  
(VISTA)-VA; National Chaplain Management Information System  
(NCMIS); Health Eligibility Records-VA; Call Detail Records-VA;  
Homeless Providers Grant & Per Diem Program Records-VA; Gulf War  
Registry-VA; Consolidated Data Information System; Disaster Emergency  
Medical Personnel System -VA (DEMPS); Automated Safety Incident  
Tracking System-VA (ASISTS); Patient Representation Program; Agent  
Orange Registry; Compliance Hotline; Spinal Cord Dysfunction Registry-  
VA; Employee Incentive Scholarship Program-VA;

1. All System of Record Identifier(s) (number):

Telephone Care and Service Records-VA; The Revenue Program – Billing and Collection Records-VA; Employee Debt Reduction Program-VA; Veterans Canteen Service (VCS) Payroll Deduction Program (PDP); National Patient Databases-VA; My HealtheVet (MHV) Administrative Records-VA

2. Name of the System of Records:

Applicants for Employment under Title 38, USC-VA; Blood Donor Information-VA; Department of Medicine and Surgery Engineering Employee Management Information Records-VA; Individuals Serving on a Fee Basis or without Compensation (Consultants, Attendings, Others) Personnel Records-VA; Motor Vehicle Operator Accident Records-VA; Non-VA Fee Basis Records-VA; Patient Medical Records-VA; Personnel Registration under Controlled Substance Act-VA; Physician, Dentist and Supervisory Nurse Professional Standards Board Action File-VA; Veteran, Employee and Citizen Health Care Facility Investigation Records-VA; National Prosthetics Patient Database-VA; Veteran, Patient, Employee and Volunteer Research and Development Project Records-VA; Health Administration Center Civilian Health and Medical program Records-VA; Voluntary Service Records-VA; Readjustment Counseling Service (RCS) Vet Center Program-VA; Community Placement Program-VA; Ionizing Radiation Registry-VA; Health Professional Scholarship Program-VA; Health Care Provider Credentialing and Privileging Records-VA; Veterans Health Information System and Technology Architecture (VISTA)-VA; National Chaplain Management Information System (NCMIS); Health Eligibility Records-VA; Call Detail Records-VA; Homeless Providers Grant & Per Diem Program Records-VA; Gulf War Registry-VA; Consolidated Data Information System; Disaster Emergency Medical Personnel System -VA (DEMPS); Automated Safety Incident Tracking System-VA (ASISTS); Patient Representation Program; Agent Orange Registry; Compliance Hotline; Spinal Cord Dysfunction Registry-VA; Employee Incentive Scholarship Program-VA; Telephone Care and Service Records-VA; The Revenue Program – Billing and Collection Records-VA; Employee Debt Reduction Program-VA; Veterans Canteen Service (VCS) Payroll Deduction Program (PDP); National Patient Databases-VA; My HealtheVet (MHV) Administrative Records-VA

3. Location where the specific applicable System of Records Notice may be accessed (include the URL):

<http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm>

Have you read, and will the application, system, or program comply with, all data management practices in the System of Records Notice(s)?	Yes
Does the System of Records Notice require modification or updating?	No
<i>(Please Select Yes/No)</i>	
Is PII collected by paper methods?	Yes
Is PII collected by verbal methods?	Yes
Is PII collected by automated methods?	Yes
Is a Privacy notice provided?	Yes
Proximity and Timing: Is the privacy notice provided at the time of data collection?	Yes
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?	Yes
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?	Yes
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?	Yes

## (FY 2011) PIA: Notice

Please fill in each column for the data types selected.

Data Type	Collection Method	What will the subjects be told about the information collection?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Verbal	The most common data types that are captured and accessed on a regular basis by authorized individuals are first and last name, middle initial, DOB, SSN, and address. This patient information falls into two classes: administrative and clinical. Clinical information is used to diagnose, prescribe treatment and follow clinically the patient through his/her health care encounters. Administrative data is used to identify the veteran (SSN), correspond to/from (name and address), and determine eligibility (patient administrative info + SSA and IRS data).	Verbally	Verbally
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Dependent data is collect during initial interviews with member upon admission	Written	Written
Service Information	Electronic/File Transfer	Military Service Information (Branch of service, discharge date, discharge type, service connection rating, medical conditions related to military service, etc). This information is collected to assess eligibility for VA healthcare benefits, type of healthcare needed.	Verbally	Written
Medical Information		The LAN is used to access the VistA-Legacy applications and meet a wide range of health care data needs. The VistA-Legacy system operates in medical centers, ambulatory and community-based clinics, nursing homes and domiciliary, and thus collects a wide range of personal medical information for clinical diagnosis, treatment, patient evaluation, and patient care. Common types of personal medical information would include lab test results, prescriptions, allergies, medical diagnoses, vital signs, etc. The information is used to treat and care for the veteran patient. Clinical information from VA and DoD is used in the diagnosis and treatment of the veteran.	Verbally	Verbally

Criminal Record Information	Verbal	VA Police VistA package stores this information to access in the effort to protect all those utilizing the VA systems.	Verbally	Verbally
Guardian Information	Verbal	Next of kin, DNR instructions, health care proxy designation. This information is used in the notification process and as required for medical decisions.	Verbally	Verbally
Education Information	Verbal	Training and Education records and employee social security numbers. Track training and education completed by employees.	Verbally	Verbally
Benefit Information	Verbal	Medical benefit determined by Eligibility from VARO	Verbally	Verbally
Other (Explain)				

Data Type	Is Data Type Stored on your system?	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	Additional Comments
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	Yes	Veteran	Mandatory	
Family Relation (spouse, children, parents, grandparents, etc)	Yes	Veteran	Voluntary	
Service Information	No	VA Files / Databases (Identify file)	Mandatory	VARO
Medical Information	Yes	Veteran	Mandatory	
Criminal Record Information	Yes	VA Files / Databases (Identify file)	Mandatory	VA Police VISTA file
Guardian Information	Yes	Veteran	Mandatory	
Education Information	Yes	Veteran	Voluntary	
Benefit Information	Yes	VA Files / Databases (Identify file)	Mandatory	Va.gov
Other (Explain)				
Other (Explain)				
Other (Explain)				

## (FY 2011) PIA: Data Sharing

Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing and its purpose.	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	VACO	Yes	Comp and Pen	Both PII & PHI	Data Use Agreement
Other Veteran Organization		No			
Other Federal Government Agency	IRS, SSA, DoD, and CMS	Yes	Data is used for income verification to determine if third party collection is possible and to determine eligibility for care.	PII	Data Use Agreement
State Government Agency		No			
Local Government Agency		No			
Research Entity		No			
Other Project / System	State HIV Database	Yes	Public health	Both PII & PHI	
Other Project / System					
Other Project / System					

## (FY 2011) PIA: Access to Records

Does the system gather information from another system?	Yes
Please enter the name of the system: CPRS/VISTA	
Per responses in Tab 4, does the system gather information from an individual?	No
If information is gathered from an individual, is the information provided:	<input type="checkbox"/> Through a Written Request <input type="checkbox"/> Submitted in Person <input type="checkbox"/> Online via Electronic Form
Is there a contingency plan in place to process information when the system is down?	Yes

## (FY 2011) PIA: Secondary Use

Will PII data be included with any secondary use request?	Yes
if yes, please check all that apply:	<input checked="" type="checkbox"/> Drug/Alcohol Counseling <input type="checkbox"/> Mental Health <input checked="" type="checkbox"/> HIV <input type="checkbox"/> Research <input type="checkbox"/> Sickle Cell <input type="checkbox"/> Other (Please Explain)
Describe process for authorizing access to this data.	
Answer: Data use agreement	

## (FY 2011) PIA: Program Level Questions

Does this PIA form contain any sensitive information that could cause harm to the Department of Veterans Affairs or any party if disclosed to the public?

No

If Yes, Please Specify:

Explain how collected data are limited to required elements:

Answer: Data is collected through system prompts

How is data checked for completeness?

Answer: System checks and user review

What steps or procedures are taken to ensure the data remains current and not out of date?

Answer: Clinical reminder queue provider at next visit

How is new data verified for relevance, authenticity and accuracy?

Answer: System checks and user review. Fields are structured for text or numerical data.

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

## (FY 2011) PIA: Retention & Disposal

What is the data retention period?

Answer: 75 years

Explain why the information is needed for the indicated retention period?

Answer: legal issues

What are the procedures for eliminating data at the end of the retention period?

Answer: Records are purged by National Archives

Where are these procedures documented?

Answer: Records management policy

How are data retention procedures enforced?

Answer: Records management

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

Yes

*Additional Information: (Provide any necessary clarifying information or additional explanation for this section.)*

Answer:

## (FY 2011) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

No

If Yes, How will parental or guardian approval be obtained?

Answer:



## (FY 2011) PIA: Security

Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured. Yes

Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.. Yes

Is security monitoring conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Is security testing conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

Are performance evaluations conducted on at least a quarterly basis to ensure that controls continue to work properly, safeguarding the information? Yes

If 'No' to any of the 3 questions above, please describe why:

Answer:

Is adequate physical security in place to protect against unauthorized access? Yes

If 'No' please describe why:

Answer:

Explain how the project meets IT security requirements and procedures required by federal law.

Answer: Continuous monitoring

Explain what security risks were identified in the security assessment? *(Check all that apply)*

- |   |   |  |
|---|---|--|
| <input checked="" type="checkbox"/> Air Conditioning Failure          | <input type="checkbox"/> Data Disclosure                                  | <input checked="" type="checkbox"/> Hardware Failure   |
| <input checked="" type="checkbox"/> Chemical/Biological Contamination | <input checked="" type="checkbox"/> Data Integrity Loss                   | <input type="checkbox"/> Identity Theft                |
| <input type="checkbox"/> Blackmail                                    | <input checked="" type="checkbox"/> Denial of Service Attacks             | <input checked="" type="checkbox"/> Malicious Code     |
| <input checked="" type="checkbox"/> Bomb Threats                      | <input checked="" type="checkbox"/> Earthquakes                           | <input checked="" type="checkbox"/> Power Loss         |
| <input checked="" type="checkbox"/> Burglary/Break In/Robbery         | <input checked="" type="checkbox"/> Eavesdropping/Interception            | <input checked="" type="checkbox"/> Sabotage/Terrorism |
| <input checked="" type="checkbox"/> Cold/Frost/Snow                   | <input checked="" type="checkbox"/> Errors (Configuration and Data Entry) | <input checked="" type="checkbox"/> Storms/Hurricanes  |
| <input checked="" type="checkbox"/> Communications Loss               | <input checked="" type="checkbox"/> Fire (False Alarm, Major, and Minor)  | <input type="checkbox"/> Substance Abuse               |
| <input checked="" type="checkbox"/> Computer Intrusion                | <input checked="" type="checkbox"/> Flooding/Water Damage                 | <input checked="" type="checkbox"/> Theft of Assets    |
| <input checked="" type="checkbox"/> Computer Misuse                   | <input type="checkbox"/> Fraud/Embezzlement                               | <input checked="" type="checkbox"/> Theft of Data      |
| <input checked="" type="checkbox"/> Data Destruction                  |   | <input type="checkbox"/> Vandalism/Rioting             |

Answer: (Other Risks)

---

Explain what security controls are being used to mitigate these risks. *(Check all that apply)*

- |  |   |   |
|--|---|---|
| <input checked="" type="checkbox"/> Access Control                                       | <input checked="" type="checkbox"/> Contingency Planning              | <input checked="" type="checkbox"/> Personnel Security                    |
| <input checked="" type="checkbox"/> Audit and Accountability                             | <input checked="" type="checkbox"/> Identification and Authentication | <input checked="" type="checkbox"/> Physical and Environmental Protection |
| <input checked="" type="checkbox"/> Awareness and Training                               | <input checked="" type="checkbox"/> Incident Response                 | <input checked="" type="checkbox"/> Risk Management                       |
| <input checked="" type="checkbox"/> Certification and Accreditation Security Assessments |   |   |
| <input checked="" type="checkbox"/> Configuration Management                             | <input checked="" type="checkbox"/> Media Protection                  |   |

Answer: (Other Controls)

---

## PIA: PIA Assessment

---

Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA.

Answer: None

---

Availability Assessment: If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization?

**(Choose One)**

- ☒ The potential impact is **high** if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.

---

Integrity Assessment: If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization?

**(Choose One)**

- ☒ The potential impact is **high** if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.

---

Confidentiality Assessment: If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization?

**(Choose One)**

- ☒ The potential impact is **high** if the loss of confidentiality could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
- ☐ The potential impact is **moderate** if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
- ☐ The potential impact is **low** if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

---

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

## (FY 2011) PIA: Additional Comments

---

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

---

(FY 2011) PIA: VBA Minor Applications

**Which of these are sub-components of your system? N/A - This PIA is for VHA LAN**

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Appraisal System	Benefits Delivery Network (BDN)	Automated Medical Information System (AMIS)290
ASSISTS	Centralized Property Tracking System	Automated Standardized Performace Elements Nationwide (ASPEN)
Awards	Common Security User Manager (CSUM)	Centralized Accounts Receivable System (CARS)
Awards	Compensation and Pension (C&P)	Committee on Waivers and Compromises (COWC)
Baker System	Control of Veterans Records (COVERS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Control of Veterans Records (COVERS)	Compensation & Pension Training Website
BDN Payment History	Control of Veterans Records (COVERS)	Corporate Waco, Indianapolis, Newark, Roanoke, Seattle (Corporate WINRS)
BIRLS	Courseware Delivery System (CDS)	Distribution of Operational Resources (DOOR)
C&P Payment System	Dental Records Manager	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Education Training Website	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Appraisal System	Enterprise Wireless Messaging System (Blackberry)
Corporate Database	Electronic Card System (ECS)	Financial Management Information System (FMI)
Data Warehouse	Electronic Payroll Deduction (EPD)	Hearing Officer Letters and Reports System (HOLAR)
EndoSoft	Eligibility Verification Report (EVR)	Inquiry Routing Information System (IRIS)
FOCAS	Fiduciary Beneficiary System (FBS)	Modern Awards Process Development (MAP-D)
Inforce	Fiduciary STAR Case Review	Personnel and Accounting Integrated Data and Fee Basis (PAID)
INS - BIRLS	Financial and Accounting System (FAS)	Personal Computer Generated Letters (PCGL)
Insurance Online	Insurance Unclaimed Liabilities	Personnel Information Exchange System (PIES)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	LGY Centralized Fax System	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	Loan Service and Claims	Purchase Order Management System (POMS)
Mobilization	Loan Guaranty Training Website	Reinstatement Entitelment Program for Survivors (REAPS)
Montgomery GI Bill	Master Veterans Record (MVR)	Reserve Educational Assistance Program CH 1607
MUSE	Mental Health Asisstant	Service Member Records Tracking System
Omnicell	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Priv Plus	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
RAI/MDS	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
Right Now Web	Rating Board Automation 2000 (RBA2000)	VA Online Certification of Enrollment (VA-ONCE)
SAHSHA	Rating Board Automation 2000 (RBA2000)	VA Reserve Educational Assistance Program
Script Pro	Records Locator System	Veterans Appeals Control and Locator System (VACOLS)
SHARE	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SHARE	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
SHARE	Spinal Bifida Program Ch 18	Veterans Service Representative (VSR) Advisor
Sidexis	State Benefits Reference System	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	State of Case/Supplemental (SOC/SSOC)	Waco Indianapolis, Newark, Roanoke, Seattle (WINRS)
VBA Data Warehouse	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Veterans On-Line Applications (VONAPP)	Web Automated Verification of Enrollment
VIC	Veterans Service Network (VETSNET)	Web-Enabled Approval Management System (WEAMS)
VR&E Training Website	Web Electronic Lender Identification	Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

(FY 2011) PIA: VISTA Minor Applications

**Which of these are sub-components of your system? N/A - This RA is for a VHA LAN system**

ASISTS	Beneficiary Travel	Accounts Receivable	Adverse Reaction Tracking
Bed Control	Care Management	ADP Planning (PlanMan)	Authorization/ Subscription
CAPRI	Care Tracker	Bad Code Med Admin	Auto Replenishment/ Ward Stock
CMOP	Clinical Reminders	Clinical Case Registries	Automated Info Collection Sys
Dental	CPT/ HCPCS Codes	Clinical Procedures	Automated Lab Instruments
Dietetics	DRG Grouper	Consult/ Request Tracking	Automated Med Info Exchange
Fee Basis	DSS Extracts	Controlled Substances	Capacity Management - RUM
GRECC	Education Tracking	Credentials Tracking	Capacity Management Tools
HINQ	Engineering	Discharge Summary	Clinical Info Resource Network
IFCAP	Event Capture	Drug Accountability	Clinical Monitoring System
Imaging	Extensible Editor	EEO Complaint Tracking	Enrollment Application System
Kernal	Health Summary	Electronic Signature	Equipment/ Turn-in Request
Kids	Incident Reporting	Event Driven Reporting	Gen. Med.Rec. - Generator
Lab Service	Intake/ Output	External Peer Review	Health Data and Informatics
Letterman	Integrated Billing	Functional Independence	ICR - Immunology Case Registry
Library	Lexicon Utility	Gen. Med. Rec. - I/O	Income Verification Match
Mailman	List Manager	Gen. Med. Rec. - Vitals	Incomplete Records Tracking
Medicine	Mental Health	Generic Code Sheet	Interim Mangement Support
MICOM	MyHealthEVet	Health Level Seven	Master Patient Index VistA
NDBI	National Drug File	Hospital Based Home Care	Missing Patient Reg (Original) A4EL
NOIS	Nursing Service	Inpatient Medications	Order Entry/ Results Reporting
Oncology	Occurrence Screen	Integrated Patient Funds	PCE Patient Care Encounter
PAID	Patch Module	MCCR National Database	Pharmacy Benefits Mangement
Prosthetics	Patient Feedback	Minimal Patient Dataset	Pharmacy Data Management
QUASER	Police & Security	National Laboratory Test	Pharmacy National Database
RPC Broker	Problem List	Network Health Exchange	Pharmacy Prescription Practice
SAGG	Progress Notes	Outpatient Pharmacy	Quality Assurance Integration
Scheduling	Record Tracking	Patient Data Exchange	Quality Improvement Checklist
Social Work	Registration	Patient Representative	Radiology/ Nuclear Medicine
Surgery	Run Time Library	PCE Patient/ HIS Subset	Release of Information - DSSI
Toolkit	Survey Generator	Security Suite Utility Pack	Remote Order/ Entry System
Unwinder	Utilization Review	Shift Change Handoff Tool	Utility Management Rollup
VA Fileman	Visit Tracking	Spinal Cord Dysfunction	CA Verified Components - DSSI
VBECS	VistALink Security	Text Integration Utilities	Vendor - Document Storage Sys
VDEF	Women's Health	VHS & RA Tracking System	Visual Impairment Service Team ANRV
VistALink		Voluntary Timekeeping	Voluntary Timekeeping National

## (FY 2011) PIA: Minor Applications

## Which of these are sub-components of your system?

1184 Web	ENDSOFT	RAFT
A4P	Enterprise Terminology Server & VHA Enterprise Terminology Services	RALS
Administrative Data Repository (ADR)	ePROMISE	Remedy Application
ADT	EYECAP	SAN
Agent Cashier	Financial and Accounting System (FAS)	Scanning Exam and Evaluation System
x Air Fortress	Financial Management System	Sentillion
Auto Instrument	Genesys	Stellant
Automated Access Request	Health Summary Contingency	x Stentor
BDN 301	ICB	Tracking Continuing Education
Bed Board Management System	KOWA	Traumatic Brain Injury
Cardiff Teleform	Lynx Duress Alarm	VA Conference Room Registration
Cardiology Systems (stand alone servers from the network)	MHTP	VAMedSafe
x CHECKPOINT	x Microsoft Active Directory	VBA Data Warehouse
Clinical Data Repository/Health Data Repository	Microsoft Exchange E-mail System	VHAHUNAPP1
Combat Veteran Outreach Committee on Waiver and Compromises	x Military/Vet Eye Injury Registry	VHAHUNFPC1
CP&E	x NOAHLINK	x VISTA RAD
Crystal Reports Enterprise	Onmicell	Whiteboard
x Data Innovations	Onvicord (VLOG)	
DELIVEREX	Optifill	
DICTATION-Power Scribe	x P2000 ROBOT	
DRM Plus	x PACS database	
DSIT	Personal Computer Generated Letters	
DSS Quadramed	PICIS OR	
EDS Whiteboard (AVJED)	x PIV Systems	
x EKG System	Q-Matic	
Embedded Fragment Registry	QMSI Prescription Processing	

(FY 2011) PIA: Final Signatures

Facility Name:

REGION 4 > VHA > VISN 02 > BATH VAMC > LAN

Privacy Officer:

Jacquelyn Filkins

607-664-4823

Jacquelyn.Filkins@va.gov

*Driscoll, RHA for J.Filkins 7/13/11*

Information Security Officer:

Audrey Ross

607-664-4507

Audrey.Ross@va.gov

*Audrey Ross 7/14/11*

System Owner/ Chief Information Officer:

Diane Niemann

518-626-6212

Diane.Niemann@va.gov

*Karen's Clancy for Diane Niemann 7/14/11*

Date of Report:

3/21/11

OMB Unique Project Identifier

029-00-02-00-01-1120-00

REGION 4 > VHA > VISN 02 > BATH

VAMC > LAN

Project Name